REMARKS

The applicant appreciates the careful examination the Examiner has given to this application and believes the claims as amended satisfy the Examiner's concerns.

With regard to Section 2 of the Action, the specification has been amended to overcome the objection of the Examiner.

With regard to Section 3 of the Action, claims 10 and 19-21 have been amended to further clarify the invention and overcome the objections of the Examiner.

Claim 10 has been amended to replace "labelling" by "labeling" on line 2 of claim 10, as requested by the Examiner.

The first claim 19 (referred to as 19a in this Office Action) has been amended by introducing additional limitations to better define the invention.

The second claim 19 (referred to as 19b in this Office Action) has been canceled.

Claim 20 has been canceled.

The first claim 21 (referred to as 21a in this Office Action) has been renumbered as claim 20 and has been amended by introducing additional limitations to better define the invention.

The second claim 21 (referred to as 21b in this Office Action) has been amended to overcome the Examiner's rejection as being indefinite by replacing "the authentication client" with "the authentication agent" and by introducing additional limitations to better define the invention.

With regard to Section 5 of the Action, the Examiner has rejected claims 13 and the second claim 19 (referred to as 19b), under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. Claim 13 has been amended by introducing additional limitations to better define the invention.

The second claim 19 (referred to as 19b) has been deleted.

With regard to Section 7 of the Action, the Examiner has rejected claims from the second claim 21 (referred to as 21b) to claim 24, under 35 U.S.C. 112, second

paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Accordingly, claims 21b to 24 have been amended to overcome the Examiner's rejection as being indefinite by replacing "the authentication client" by "the authentication agent" and by introducing additional limitations to better define the invention.

With regard to Section 10 of the Action, the Examiner has rejected claims 15, 17 and 24 under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,212,561 to Sitaraman et al. (Sitaraman).

Claim 15 has been amended by introducing additional limitations to better define the invention.

Claim 15 as amended provides an integrated access device, for placement between a user network and an external network, the external network having an access rights authentication server. The integrated access device comprises a user network interface for operatively connecting to a plurality of user networks to receive data units from the plurality of user networks; an authentication agent, operatively connected to the user network interface for locally authenticating, authorizing and forwarding data units received from the plurality of user networks; an external network interface, operatively connected to the authentication agent, for forwarding data units locally authorized by the authentication agent to the external network; and means for communicating with the authentication server of the external network.

Advantageously, as amended in claim 15, local authentication of the data units at the integrated access device prevents unnecessary traffic interchange between the user networks and the authentication server of the external network, accordingly preventing unnecessary traffic to consume precious bandwidth in the access network. Further, the means for communicating with the authentication server of the external network comprises means for determining whether the data unit is eligible for transmission from the integrated access device to the authentication server of the external network and, if the data unit is not eligible for transmission, the integrated access device drops the data unit, this in turn, reduces unnecessary traffic through from traversing the access network.

In contrast, U.S. Patent 6,212,561 (Sitaraman) teaches an apparatus for providing the owners of domain sites on a computer network or the owners of private

remotely accessible intra networks the capability to force authorized users to disconnect from any open connections to other public or private domains or networks before a connection with the owners domain or network can be established. This forced sequential access of a specified domain or network is accomplished by inserting a sequential-only attribute into the service profile for a specified user. Upon the user initiating a log-on sequence through an access point, the user's service profile is pulled from a memory bank and an assessment is made as to whether or not the sequential-only attribute exists for the desired specified domain or network to be accessed. If the attribute exists and the user has potentially concurrent connections outstanding, the user is alerted of the mandatory requirement to disconnect from these open connections before proceeding further with desired specified domain or network connection.

As a result, Sitaraman's apparatus doesn't provide means for controlling the traffic traversing the access network, hence, allowing unnecessary traffic to occupy precious bandwidth in the access network in contrast to the present invention.

Claims 17 and 24 are dependant on the amended claim 15 and include further limitations.

With regard to claims 17 and 24 please note the following:

Claim 17 has been amended to correct words misspelling, and

Claim 24 has been amended to overcome the Examiner's rejection under 35 U.S. 112, second paragraph, as being indefinite by replacing "the authentication client" by "the authentication agent".

It is respectfully submitted that these rejections of the Examiner have been traversed.

With regard to Section 12 of the Action, the Examiner has rejected claim 1-4, 6 and 11-13 under 35 U.S.C. 103(a) as being unpatenable over U.S. Patent 6,584,505 to Howard et al. (Howard) in view of "Remote Authentication Dial In User Service (RADIUS)" by Rigney et al. (Rigney).

Claim 1 has been amended by introducing additional limitations to better define the invention.

Claim 1 as amended provides a distributed subscriber management method for controlling user authentication at an access control node located between a plurality of user networks and an access network, the access network being connected

to an external network having an access rights authentication server. The method comprises the steps of receiving, at the access control node operatively connected to the plurality of user networks, a data unit from a user located on one of the plurality of user networks; and determining whether the data unit requires authentication. If the data unit requires authentication, determining whether authentication locally stored on the access control node. If authentication locally stored on the access control node, authenticating the data unit to prevent unnecessary traffic interchange between the access network and the plurality of user networks from consuming precious bandwidth in the access network. If authentication is not locally stored on the access control node, determining whether the data unit is eligible for transmission to the external network. If the data unit is eligible for transmission, transmitting said data unit from the access control node to the authentication server of the external network.

The method in the amended claim 1 comprises steps for controlling user authentication, including steps for determining whether local authentication can be provided at the access control node; determining whether the data unit is eligible for transmission from the access control node to the authentication server of the external network; transmitting the data unit to the authentication server of the external network; receiving, at the access control node, an authentication message for the data unit from the authentication server to permit the user to access the external network; and storing the authenticated data units in the local authorization table on the access control node for local authentication, as a result, the method allows for managing the traffic traversing the access network and preventing unnecessary traffic from occupying extra bandwidth in the access network.

In contrast, U.S. Patent 6,584,505 (Howard) teaches a method of granting access to a network server, the method comprising receiving, at an authentication server, a request to authenticate a user, wherein the request is generated by the network server to which the user is attempting to gain access; and determining whether the user was already authenticated by the authentication server. If the user was already authenticated by the authentication server, notifying the network server that the user is authenticated; and if the user was not already authenticated by the authentication server, then retrieving login information from the user, wherein the login information is not communicated through the network server, authenticating the user by comparing the retrieved login information with authentication information maintained by the

authentication server, notifying the network server that the user is authenticated if the retrieved login information matches the authentication information.

The "Remote Authentication Dial In User Service (RADIUS)" (Rigney) is a client-server operational model. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response that is returned. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user.

U.S. Patent 6,584,505 (Howard) in combination with "Remote Authentication Dial In User Service (RADIUS)" (Rigney) authentication scheme allows unauthorized traffic to fully traverse the access network and hence, generates unnecessary traffic, which is transmitted over the access network consuming extra bandwidth. Accordingly, Howard in combination with Rigney will not lead to the current invention as formulated in the amended set of claims.

With regards to Sections 13 to 15 of the Action, please note that claims 5 and 7-9 have been amended by introducing additional limitations to better define the invention.

With regards to Sections 16 to 24 of the Action, please note that claims 10, 14, 16, 18, the first claim 19 and the second claim 19 (referred to as 19a and 19b respectively), 20, the first claim 21 and the second claim 21 (referred to as 21a and 21b respectively), 22, and 23 either have been amended by introducing additional limitations to better define the invention or canceled.

The Examiner is requested to respectfully reconsider this application with regard to the amendments to the claims presented above and the above arguments with a view to considering the claims favorably for allowance.

The Commissioner is hereby authorized to deduct any prescribed fees for these amendments from our Company's **Deposit Account No. 501832.**

Yours truly,

SKEMER, TERRY

By: _____

Victoria Donnelly
Patent Agent
Reg. No. 44,185

VD/OM.

C/o TROPIC NETWORKS INC.,
Intellectual Property Department
135 Michael Cowpland Drive
Kanata, Ontario, Canada.
K2M 2E9

Date: October 22, 2004
Telephone: (613) 270-6026
FAX: (613) 270-9663
E-mail: Victoria.Donnelly@tropicnetworks.com

CERTIFICATE OF MAILING

I hereby certify that this paper (21 pages) is being sent by FEDEX Courier service in a package having a tracking No. 7919 6230 2924 to the following address:

Patent and Trademark Office
2011 South Clark Place
Customer Window, Mail Stop: Non-Fee Amendment

Crystal Plaza Two, Lobby, Room 1B03

Arlington, VA 22202

Omayma E. Moharram, Ph.D., P.Eng.
Patent Engineer, Tropic Networks Inc.
135 Michael Cowpland Drive
Kanata, Ontario, Canada.
K2M 2E9
Date: October 22, 2004
Telephone: (613) 270-6942
Fax: (613) 270-9663
E-mail: Omayma.Moharram@tropicnetworks.com